

REMARKS

Claims 1-6 and 22-31 have previously been canceled. Claims 7-21 and 32-40 are still pending in this application.

Rejections under Section 103

The Examiner has rejected claims 7-21 and 32-40 under section 103 as being unpatentable over *Barnes et al.* in view of *O'Mahony*, "Electronic Payment Systems" (*O'Mahony*). Although the Examiner's arguments have been carefully considered, Applicant respectfully traverses this rejection as explained below.

The Cited Art Distinguished Over Independent Claims 7, 20, 21 and 32

The present office action agrees (and in accordance with an earlier telephone interview) that *Barnes et al.* does not teach or suggest a trusted party authenticating a user during a transaction. Accordingly, the present action relies upon *O'Mahony* to disclose payment systems where a trusted party verifies consumers and authenticates financial transactions. Respectfully, it is submitted that the various payment schemes (especially First Virtual, CARI and CyberCash) disclosed in *O'Mahony* are quite different from the currently claimed invention.

Claims 7, 20, 21 and 32 have been amended to require that it is the issuer of the account that takes responsibility for verifying the identity of the customer as the owner of the account during a registration process. It is also the issuer that compares the password received from the customer with the originally recorded password for that account. The specification broadly describes "issuer" at pages 8 and 9.

Because the issuer is the organization that maintains the account owned by the user, there are advantages in having the issuer enroll the user in the authentication system. The issuer already holds a wealth of information about a prospective user and can use this information to verify an identity of such a user much better than other organizations that do not have a prior relationship with the user. For example, the issuer has a cardholder system 110 that includes account information and services utilized by a cardholder. An identity authentication database 116 contains information that the issuer already has on file regarding a cardholder and is used by the issuer to enroll cardholders and to verify their identity. Pages 9-10. An issuer can also provide identity authentication policies and other information to be used in a cardholder identity

verification process. Cardholder authentication information includes information such as business identification, country code, card account number, card expiration date, cardholder name, issuer-specific authentication data, mother's maiden name, billing address, shipping address, Social Security number, telephone number, account balance, transaction history, driver license number, etc.

The issuer is able to use the above information it already holds to verify the identity of a prospective user during registration and to provide a solid assurance that the password associated with that account is being provided to the person that the prospective user claims to be. An organization other than the account issuer simply does not have access to this information and cannot guarantee to the same level that the person to whom is issued a password is the person they claim to be. The systems described in *O'Mahony* (especially First Virtual, CARI and CyberCash), are deficient in that they do not teach or suggest that the issuer of the user account is the organization that registers the user and compares the passwords during a transaction.

First Virtual

Figure 4.2 at page 66 of *O'Mahony* illustrates the First Virtual authentication system. A buyer (analogous to an entity or user) is buying goods from a merchant (analogous to a third party); a First Virtual server authenticates the buyer's identifier for the merchant. (The identifier is a so-called "VirtualPIN" or password.) First Virtual does not issue a credit card to the buyer and does not issue an account to the buyer that the buyer is attempting to authenticate; it simply is not an issuer. First Virtual is an unrelated company that performs the service of authentication for the buyer and merchant. In fact, a credit card company views First Virtual as a merchant, not as an issuer (third to last paragraph).

Because First Virtual is not an issuer it performs virtually no verification of the buyer's identity when the buyer registers. A buyer registers with First Virtual by forwarding his credit card details and in return receiving a password (third paragraph). There is no verification of the buyer's identity being performed before the buyer can receive a valid password from First Virtual. By contrast, independent claims 7, 20, 21 and 32 require that the issuer verify the identity of the entity as the owner of the account during registration or enrollment. Because First Virtual does not verify the buyer's identity during registration (as is required by the independent claims), the authentication system of First Virtual cannot guarantee the identity of the buyer. For example, the article states "the system is not entirely fraudproof" (first paragraph) and that

"bogus purchases can be made from then until such time as the VirtualPIN is blacklisted (fifth paragraph from the end). Further, "a stolen credit card number could be used to set up VirtualPINs associated with e-mail addresses controlled by the attacker" (fourth paragraph from the end).

Stolen credit card numbers can be used to set up fake passwords because there is no verification of the buyer's identity during registration (because First Virtual does not have access to an issuer's user account information). The inventions of claims 7, 20, 21 and 32 nearly guarantee that stolen numbers cannot be used to set up fake passwords because the issuer verifies the user's identity during registration. Further, it is First Virtual that compares the passwords at the request of the merchant (fifth paragraph); it is not the issuer of the credit card account that does the comparison as is required by the independent claims.

CARI

Figure 4.4 at page 69 and figure 4.5 at page 71 of *O'Mahony* illustrate registration and purchase using the CARI authentication system. A consumer (analogous to an entity or user) is buying goods from a merchant (analogous to a third party); a CARI machine authenticates the consumer's virtual credit card number for the merchant. (The virtual credit card number or "VCC" is a random number assigned by CARI; we refer to it as a password.) CARI does not issue a credit card to the consumer and does not issue an account to the consumer that the consumer is attempting to authenticate; CARI simply is not an issuer. CARI is an unrelated company that performs the service of authentication for the consumer and merchant.

Because CARI is not an issuer it performs virtually no verification of the consumer's identity when the consumer registers. To register (section 4.4.2), a user enters personal details such as name, e-mail address, shipping address and telephone number, and then provides credit card details to CARI by telephone. The user is then assigned a password which is then activated. But, there is no verification of the user's identity being performed by the account issuer before the user can receive a valid password from CARI. By contrast, independent claims 7, 20, 21 and 32 require that the issuer verify the identity of the entity as the owner of the account during registration or enrollment. At the end of section 4.4.2 it is stated that "the real card is verified" but presumably this can only mean checking the name on the credit card with the name previously provided. CARI cannot perform extensive verification of the user's identity because it does not have access to the wealth of information that an account issuer has.

A stolen credit card can be used to set up a fake user in the CARI system because there is no verification of the user's identity during registration by an issuer (because CARI is not an issuer and does not have access to a credit card issuer's account information). A thief can steal a card and then supply the appropriate personal details using the name on the card. Because CARI is not an issuer and cannot verify the user's identity during registration (as is required by the independent claims), the authentication system of CARI cannot guarantee the identity of the user. The inventions of claims 7, 20, 21 and 32 nearly guarantee that stolen numbers cannot be used to set up fake users because the issuer verifies the user's identity during registration. Further, it is CARI that compares the passwords at the request of the merchant (section 4.4.4); it is not the issuer of the credit card account that does the comparison as is required by the independent claims.

Further, claim 7 requires that the issuer receive from said customer during the online transaction an identity authenticating password, and that the issuer notify "said third party over said network during said online transaction." CARI discloses an NFS client (that compares the passwords) that is not on line and does not communicate with the consumer. Claim 20 requires that the issuer request and verify a password from the customer; claim 21 requires that the customer receives a request from an access control server of the issuer to enter a password; and claim 32 requires that the customer supply a password to a computer of the issuer during a financial transaction. CARI does not disclose that the consumer communicates directly with CARI. Further, CARI cannot authenticate a user to a merchant on line and in real time because it sends order information "to the merchant via fax, secure ftp, encrypted e-mail, or a dial-up line." Even if ftp, e-mail or a dial-up line is used, authentication cannot happen in real time because a connection to the merchant must be established; there is no existing online connection such as would exist in the case of an Internet connection.

CyberCash

The CyberCash system described in section 4.6 likewise does not disclose an account issuer that verifies the identity of the customer during a registration process and obtains a password. Relevant parts of the CyberCash system are shown in Figures 4.10 and 4.11. As described, CyberCash does not rely upon a customer registration process to establish the identity of the customer and to associate a password with that account. By contrast, CyberCash relies upon digital signatures. In fact, as described in the first two paragraphs of section 4.6.3, it would be possible for an unscrupulous party to simply sit down at a legitimate customer's computer and

engage in a financial transaction because no password is required of the user in order to engage in a transaction. The customer's credit card is registered with the software previously, but such a process does not include verifying the customer's identity as the owner of a financial account.

Therefore, the CyberCash system does not teach or suggest verifying the identity of a customer as the owner of an account during a registration process, but rather teaches a more complex scheme relying upon digital signatures.

The Remaining Payment Systems

None of the other remaining payment systems described in the other sections of Chapter 4 teach or suggest that the issuer of an account verifies during a registration process the identity of the customer as the owner of the account. Section 4.5 discusses SSL that does not involve an account issuer as a trusted party. The iKP system of section 4.7 relies upon public-key cryptography; section 4.8 is based upon the 3KP technique of section 4.7. The SET system of section 4.9 is also based upon public-key cryptography. The electronic check systems of Chapter 5 all involve electronic checks and likewise do not disclose an issuer verifying the identity of the customer during a registration process.

Dependent Claims

Claim 9 requires determining if a user is enrolled by looking at a database of enrolled accounts; the cited art does not disclose checking to see if a user is enrolled before performing the authentication process. Claim 14 requires that the issuer or an access control server of the issuer sign a transaction receipt using a signature key; again, the cited art does not disclose that it is the issuer that authenticates a user and thus is able to provide a signed transaction receipt.

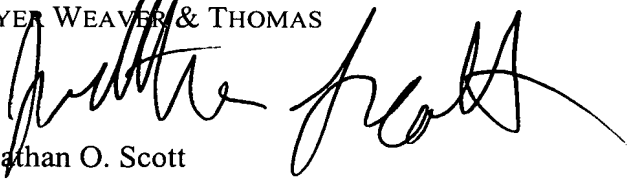
Dependent claims 37-40 all require that the authentication request from the third party to the issuer is routed via a computer of the user. Such features are not taught or suggested in the art of record. The advantage of these features is that as long as the user's computer has connected to a merchant computer over an online connection, it is convenient for the merchant computer to query the issuer computer via the user's browser. The issuer computer is then conveniently connected to the user computer and can ask for the identity-authenticating password.

Dependent claim 10 requires that it is determined whether the user is registered or enrolled before sending a request from the third party to the issuer for authentication. Such

features are not taught or suggested in the art of record. Depending upon the embodiment, the specification discloses that this determination can occur by checking a directory server (or other database) to see if a user's account number is present in a list of enrolled users, or by checking to see if the user computer has special software installed. The advantage of these features is that a quick check for an enrolled user can avoid a time-consuming and error-prone authentication process for users that are not enrolled.

Reconsideration of this application and issuance of a Notice of Allowance at an early date are respectfully requested. If the Examiner believes a telephone conference would in any way expedite prosecution, please do not hesitate to telephone the undersigned at (612) 252-3330.

Respectfully submitted,
BEYER WEAVER & THOMAS



Jonathan O. Scott
Registration No. 39,364

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778

Telephone: (612) 252-3330
Facsimile: (612) 825-6304